County Technical Assistance Service
INSTITUTE for PUBLIC SERVICE

February 05, 2025

Public Access to Records

Dear Reader:

The following document was created from the CTAS website (ctas.tennessee.edu). This website is maintained by CTAS staff and seeks to represent the most current information regarding issues relative to Tennessee county government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with county government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other CTAS website material.

Sincerely,

The University of Tennessee
County Technical Assistance Service
226 Anne Dallas Dudley Boulevard, Suite 400
Nashville, Tennessee 37219
615.532.3555 phone
615.532.3699 fax
www.ctas.tennessee.edu

Public Access to Records 3
The Freedom of Information Act (FOIA) 3
Tennessee Public Records Statutes 3
Who Has Access? 4
How Should Access Be Provided? 4
Limiting Risks 5
Providing Copies of Public Records 5
Charging for Copies 6
Records with Commercial Value 6
Special Issues in Providing Access to Court Records 7
Expunging Court Records 7
Providing Access to Records in Non-Paper Formats 8
Providing Access to Electronic or Computerized Records 8
Remote Access to Computerized Records 9
Denial of Access to Public Records—Liability 10
To What Records Is the Public Entitled Access? 10
Confidential Records 11
Maintenance of Confidentiality 13
Special Considerations and Specific Types of Confidential Records 13
Personally Identifying Information 13
Motor Vehicle Registration Records 14
Vital Records 15
Law Enforcement Personnel Records 15
Computerized Data Breaches 16
Domestic Violence Prevention and Protection Documents 16
County Hospital and Health Department Records and Ambulance Records 16
HIPAA 17
Credit Card Numbers and Credit Reports 18

Public Access to Records

Reference Number: CTAS-210

Modern laws requiring public access to government records began to surface in the United States in the 1950s. But the concept of openness in government goes back to the start of our nation. Certain of the founding fathers placed a great deal of importance on the need for citizens to be informed about the activities of their government. However, even the most visionary of the founding fathers probably did not anticipate the depth and breadth of information held by the government today. The struggle to balance the right of the public to access government records with the increasing desire to protect privacy and confidentiality gets more difficult each year. While new technologies have enhanced our ability to manage data and information, they have also created new fears about abuse of personal and confidential information. The sword of liability can cut both ways. There are potential liability concerns for refusing access to records that are public and for disclosing confidential information. For these reasons, it is important for the custodian of public records to have a good understanding of the public's right to access government records and the limitations on that right.

The Freedom of Information Act (FOIA)

Reference Number: CTAS-1152

During the "atomic age" following WWII, a strong movement began on the state and federal level to allow the public access to information about what the government was doing and to files that the government had collected about individual citizens. This push resulted in the passage of "open records" laws in many states during the 1950s and culminated in the passage of the Freedom of Information Act at the federal government level[1]. Tennessee was among those states passing an open records law in the 1950s.[2]The specifics of our state laws will be discussed shortly, but first it is useful to make a few brief points about the Freedom of Information Act. "The Freedom of Information Act (FOIA)[3]was passed by Congress in 1966 and amended in 1974. Based on the premise argued by Madison and Hamilton that openness in government will assist citizens in making the informed choices necessary to a democracy, FOIA creates procedures whereby any member of the public may obtain the records of the agencies of the federal government."[4]

The main thing county officials need to know about the FOIA is that it applies to *agencies of the federal government.*[5]The Freedom of Information Act does NOT apply to county governments. As a county records custodian, you need to be aware of the FOIA because citizens may try to assert their rights to county government records under that act due to confusion as to which laws apply. Different policies and procedures apply to federal offices under the Freedom of Information Act that are not included in the Tennessee public records statutes that apply to your office. Under the FOIA, citizens may request a federal agency covered by the act to perform searches of its records to locate certain information and then disclose the information, providing copies to the person making the request (subject to certain fees). As will be seen, Tennessee statutes allow broad access to public records, but they do not generally require local officials to perform searches or create new reports or responses to requests if those reports are not already a part of the office records.

---

[1] *Using the Freedom of Information Act, a Step-by-Step Guide*, an American Civil Liberties Union Publication.

[2] T.C.A. § 10-7-503, which makes most state and local government records in Tennessee public, passed in 1957.

[3] 5 U.S.C.A. § 552(a).

[4] *Using the Freedom of Information Act, a Step-by-Step Guide*, an American Civil Liberties Union Publication.

[5] 5 U.S.C.A. § 552(f).

Tennessee Public Records Statutes

Reference Number: CTAS-1153

The public records statutes that do apply to county offices are found in Title 10, Chapter 7, Part 5 of the *Tennessee Code Annotated*. The starting point for a discussion of the law in this area is the declaration found in T.C.A. § 10-7-503, that government records are open to public inspection. It reads as follows:

> ... [A]ll state, county and municipal records ... except any public documents authorized to be destroyed by the county public records commission in accordance with § 10-7-404, shall at all times, during business hours, be open for personal inspection by any citizen of Tennessee, and those in charge of such records shall not refuse such right of inspection to any citizen, unless otherwise provided by state law.[1]

This statute has been construed broadly by the both the state attorney general and the Tennessee judiciary.[2]The legislature made it clear that its intent in passing this law was to "...give the fullest possible public access to public records" and it instructed the courts to exercise whatever remedies are necessary to ensure that purpose is fulfilled.[3]The courts have ruled that a "presumption of openness" exists with government documents.[4] That is not to say that public access is totally without limitation however.

---

[1]T.C.A. § 10-7-503.

[2]See generally, *Memphis Publishing Co. v. Holt*, 710 S.W.2d 513 (Tenn. 1986).

[3]T.C.A. § 10-7-505(d).

[4]*Griffin v. City of Knoxville*, 821 S.W.2d 921, 924 (Tenn. 1991).

Who Has Access?

Reference Number: CTAS-1154

The statute states that records must be open for inspection by any "citizen" of Tennessee. In keeping with the legislative intent to provide for liberal public access to government records, the Tennessee Supreme Court has determined that the word "citizen" includes convicted felons incarcerated as inmates within the Tennessee prison system.[1]Although certain rights are stripped from individuals when they are convicted of a felony (i.e. voting, ability to hold public office), the court concluded that neither the Tennessee Public Records Act nor any other statute prevented a convicted felon from seeking access to public records. Neither should access be denied to anyone else who appears to be a citizen of this state.

The law is not as generous with non-residents. Since the statute states that it grants public access to "any citizen of Tennessee," the Tennessee attorney general has opined that public officials may deny requests for copies of public records based on the lack of state citizenship.[2] Since there is no fundamental federal right to access of government records and since Tennessee's laws provide access only to state citizens, the attorney general reached the conclusion that it is not a violation of the privileges and immunities clause of the United States Constitution to deny access to persons making requests from other states for Tennessee records. Keep in mind that although the act does not affirmatively require disclosure of public records to non-citizens, neither does it prohibit the release of public records to non-citizens.[3]It is within the discretion of the official who has custody of the records to determine whether or not access will be provided to non-citizens. It is the recommendation of CTAS that offices should develop a written policy in that regard and enforce it consistently.

---

[1]*Robin M. Cole v. Donal Campbell*, 968 S.W.2d 274 (Tenn. 1998).

[2]Op. Tenn. Att'y Gen. No. 99-067 (March 18, 1999) re-affirmed by Op. Tenn. Att'y Gen. No. 01-132 (August 22, 2001).

[3]Op. Tenn. Att'y Gen. No. 99-067 (March 18, 1999).

How Should Access Be Provided?

Reference Number: CTAS-1155

The law states that records shall be open to inspection "during business hours." Every effort should be made to provide reasonable accommodation to parties requesting access to records; however, providing

this service need not prevent the performance of other duties of the office. A request to see every record of an office and make a photocopy of each of them could obviously bring the entire operation of an office to a halt. For this reason, the official who has custody of the records is also authorized by law to adopt and enforce reasonable rules governing the making of extracts, copies, photographs or photostats of the records.[1]These regulations should be reasonable and not interfere with the intent of the legislature to provide broad public access to records. The official with custody of the record should strive to balance the right to access records with his or her responsibility to preserve and protect the records. Regulations should be tailored to accommodate requests in a timely manner while allowing for the continued efficient functioning of the office and for the preservation and security of the records. Regulations that are intended to frustrate the ability of a citizen to access records will likely be found unreasonable and struck down by the courts. The county public records commission may serve as a valuable resource in developing and drafting these regulations.

Although there is little legal authority in this area, the following are some examples of regulations that would likely be found reasonable by a court:

- Establishing that copies of records would be provided within a reasonable time period (for example: the next business day for small requests and within five business days for larger requests);
- Prohibiting the inspection and copying of records by citizens without supervision of the official or an employee of the office; and
- Prohibiting the handling of older bound volumes or other fragile records by anyone other than an employee of the office so long as the information in the records is still provided in a usable format.

Another possible regulation could provide that requests for inspection of a large number of records would be accommodated only by appointment pursuant to a written request. In a 2001 opinion, the attorney general was asked to consider a very similar requirement. In opinion 01-021, the attorney general found that there was no clear answer to the question. While the public records laws are to be interpreted to allow the fullest possible access, this should not lead to absurd results. The attorney general opined that if a citizen challenged a requirement to set an appointment to view records, a court might not find this requirement to be tantamount to a denial of access if the agency could articulate a reasonable basis for requiring the appointment. Absent a legitimate reason, the court may conclude the requirement of an appointment was merely being used to delay access to the records.[2] This opinion therefore appears to support the idea that local officials can implement reasonable regulations so long as there is a clear, articulated reason for the regulation that relates to goals of records management. .

---

[1] T.C.A. § 10-7-506(a).

[2] See Op. Tenn. Att'y Gen. No. 01-021 (February 8, 2001).

Limiting Risks

Reference Number: CTAS-1156

Be aware that there is a danger of theft, vandalism, or damage by negligence inherent in allowing a member of the public access to government records. There is a profitable market out there for certain historical manuscripts. Across the country, government records are disappearing from government offices and reappearing for sale in antique stores, flea markets, speciality shops, or Internet auction sites. To prevent theft or vandalism, someone from your office should supervise the person accessing the records or, at a minimum, the person accessing the records should be required to examine them in an open area where abuse of the records or attempted thefts will be noticed. If county records have been lost in the past and are discovered in someone's possession, the Tennessee Code, in Section 39-16-504, grants statutory authority to counties to initiate judicial proceedings to reclaim lost, stolen, or otherwise misappropriated records.

Providing Copies of Public Records

Reference Number: CTAS-1157

In all cases in which a person has the right to inspect public records, he or she also has the right to take extracts or make copies of the record, or to make photographs or photostats of the record while it remains

in the possession, custody, and control of the official who has lawful custody of the record.[1] In 1999, the attorney general interpreted this to mean that the Tennessee Public Records Act does not require a public official to make copies and send them to anyone regardless of whether or not they are a citizen of Tennessee.[2] However, this opinion is limited by a subsequent court decision. In the case of *Waller v. Bryan*,[3] the Tennessee Court of Appeals required public officials to make public records available to members of the public who could not visit the official's office under certain circumstances. In that case, an inmate appealed the ruling of a chancellor that he was not entitled to requested records which were in the possession of a police department. The local government refused to make copies of the requested records and mail them to the inmate. Obviously, his circumstances did not allow him to appear in person to inspect the records and make a copy. The Court of Appeals held that as long as a citizen can sufficiently identify the requested records so that the government office knows which records to copy, the official should comply with the records request. To refuse to do so merely because the citizen could not appear in person would, in the words of the court, "place form over substance and not be consistent with the clear intent of the Legislature."[4] The court observed that a requirement to appear in person would not only limit access to records by inmates, but also all those Tennessee citizens who were prevented by health problems or other physical limitations from appearing at the government office.

---

[1] T.C.A. § 10-7-506(a).
[2] Op. Tenn. Att'y Gen. No. 99-067 (March 18, 1999).
[3] *Waller v. Bryan*, 16 S.W.3d 770, (Tenn. App. 1999).
[4] Waller, at 773.

Charging for Copies

Reference Number: CTAS-1158

The Office of Open Records Counsel, created in 2008, was charged with developing a schedule of reasonable charges which may be used as a guideline in establishing charges or fees, if any, to charge a citizen requesting copies of public records. On October 1, 2008, the Office of Open Records Counsel issued its Schedule of Reasonable Charges for Copies of Public Records. Records custodians are authorized by T.C.A. § 10-7-503(a)(7)(C)(i) to charge reasonable costs consistent with the schedule. The schedule, together with instructions for records custodians, can be found on the website of the Office of Open Records Counsel. Charges established under separate legal authority are not governed by the schedule, and are not to be added to or combined with charges authorized under the schedule. Questions regarding the schedule should be directed to the Office of Open Records Counsel.

Records with Commercial Value

Reference Number: CTAS-1159

The legislature has recognized that in certain circumstances, a governmental agency may expend a great deal of money developing a record with great commercial value. That record in turn may then be requested by a company who only has to pay a small fee for a reproduction of the information which may be used to generate significant amounts of revenue. Therefore, the legislature in 2000 amended T.C.A. § 10-7-506 to add provisions that protect the investment of government resources specifically in computer generated maps or geographic information systems. These systems are expensive to develop and have numerous profitable commercial applications once the data is developed. Private entities could acquire a copy of the data and regular updates for practically no cost then profit greatly by selling subscriptions to the data. For this reason, the legislature allowed governments to also recover a portion of the actual development and maintenance costs when providing copies of computerized mapping systems or data to persons other than the news media or individuals for non-business use. While this general statute is limited to electronic geographic records, an additional statute applicable only to court clerks offices in Knox and Shelby counties allows those officials to charge a fee not to exceed $5 for computer searches for any public record having a commercial value.[1]

---

[1] T.C.A. § 8-21-408.

Special Issues in Providing Access to Court Records

Reference Number: CTAS-1160

Court records can be a little different from most of the records in other county offices in that they are created by parties of the case who need access to the records on an on-going basis during litigation. The evidence and discovery materials in the cases are not created by the clerk, but merely held for use by the parties. For this reason, though case files are technically public records, special provisions may apply. The United States Supreme Court has stated that "every court has supervisory power over its own records and files."[1] In Tennessee, the Court of Criminal Appeals has similarly ruled that "a trial court has the inherent authority to determine the custody and control of evidence held in the clerk's office."[2]These case files, while in the court clerk's office, will usually be open to the public.[3] This public right of access is rooted in the First Amendment and in the common law, but is a qualified right.[4] Since this right is qualified and not absolute, it is subject to the court's discretion on a particular matter.[5] Therefore, unless there is a statute making a record confidential or a clear court directive sealing records or prohibiting public access to the records, the public may access case files. If the court seals a record, it becomes confidential and free from public scrutiny.[6] This power is not unlimited. The records may only be sealed when "interests of privacy outweigh the public's right to know."[7] If parties to litigation approach a clerk with concerns about public access to materials included in case files, the clerk should direct the parties to petition the judge to order such records sealed from public access. Additionally, as parties to litigation may need extended access to and use of case records, courts may also adopt rules to authorize that pleadings and exhibits may be withdrawn by parties to the case or their legal representatives.[8]

---

[1] *Nixon v. Warner Communications*, 435 U.S. 589, 98 S.Ct. 1306 (1978).

[2] *Ray v. State*, 984 S.W.2d 236, 238 (Tenn. Crim. App. 1997).

[3] *Smith v. Securities and Exchange Commission*, 129 F.3d 356, 359 (6th Cir. 1997). See also Op. Tenn. Att'y Gen. No. 02-075 (June 12, 2002).

[4] *Ballard v. Herzke*, 924 S.W.2d 652, 661-662 (Tenn. 1996).

[5] *Ray v. State*, at 238.

[6] *Knoxville News-Sentinel v. Huskey*, 982 S.W.2d 359, 362 (Tenn. Crim. App. 1998)

[7] In re Knoxville News-Sentinel, 723 F.2d 470, at 474 (6th Cir. 1983).

[8] Op. Tenn. Att'y Gen. No. 02-075 (June 12, 2002).

Expunging Court Records

Reference Number: CTAS-1161

Several statutes in Tennessee law provide for parties to have records of judicial proceedings involving them expunged from the records of the court and certain other offices.

The basic statute for expunction of criminal offense records is found in T.C.A. § 40-32-101. This statute allows individuals to have their records expunged if they are not convicted of any crime. The statute also allows for expungements of charged offenses if the individual was not convicted of the charged offense, even if they are convicted of another offense, so long as the only offense the individual was convicted of was a traffic offense. Additionally, subsection (j) allows an individual to apply for expungement of records from electronic databases relating to the person's arrest, indictment, charging instrument, or disposition for any charges other than the offense for which the person was convicted. Finally, subsection (g) allows for the expungement of certain less serious convictions under certain circumstances if the individual pays the required statutory fees.

The law provides that the record to be expunged "does not include arrest histories, investigative reports, intelligence information of law enforcement agencies, or files of district attorneys general that are maintained as confidential records for law enforcement purposes and are not open for inspection by members of the public and shall also not include records of the department of children's services or department of human services that are confidential under state or federal law and that are required to be maintained by state or federal law for audit or other purposes." Court cases have also determined that

physical evidence is not addressed by the expungement statutes; and therefore, cannot be expunged. State v. Powell, 1999 WL 512072 (Tenn. Ct. App. July 21, 1999, permission to appeal denied January 24, 2000).

In cases of judicial diversion, there is separate statutory authority for expunging records. T.C.A. § 40-35-313. In those circumstances, a person who had charges dismissed through judicial diversion may apply to the court to expunge all official records other than certain non-public records that are kept solely to determine whether the person is eligible for diversion in the future. The application for expungement shall contain a notation by the clerk evidencing that all court costs are paid in full, prior to the entry of an order of expungement. If the court determines, after hearing, that the charges against such person were dismissed and the proceedings discharged, it shall enter such order. The effect of such order is to restore the person, in the contemplation of the law, to the status the person occupied before such arrest or indictment or information.

Other statutes authorize expunction in cases that were dismissed through pre-trial diversion under a memoranda of understanding, T.C.A. § 40-15-105, or in cases where the governor declares the defendant exonerated. T.C.A. § 40-27-109.

In cases where the criminal record is expunged, certain information must be reported to the Tennessee Bureau of Investigation (TBI) to be maintained in its expunged criminal offender and pretrial diversion database. T.C.A. § 38-6-118.

In addition to courts with criminal jurisdiction, the primary statute on expunging criminal offenses explicitly states that it applies to juvenile courts. T.C.A. § 40-32-101(a)(4). Additionally, Juveniles who have their driving record suspended can apply to have that record expunged once they reach 18 years of age and have their license reinstated. T.C.A. § 55-10-711.

Outside of the criminal setting, parties to any divorce proceeding, who have reconciled and dismissed their cause of action, may file an agreed sworn petition signed by both parties and notarized, requesting expungement of their divorce records. T.C.A. § 36-4-127. Upon the filing of such petition, the judge shall issue an order directing the clerk to expunge all records pertaining to such divorce proceedings, once all court costs have been paid. The clerk shall receive a fee of $50 for performing such clerk's duties under this section.

Other less commonly used statutory provisions allow for the expunction of affidavits of heirship from the register of deeds office, T.C.A. § 30-2-712, and records of proceedings related to the appointment of a fiduciary where none was appointed. T.C.A. § 34-1-124. Also, records of military discharge may be expunged by registers of deeds from their records upon application by proper parties T.C.A. § 10-7-513.

Providing Access to Records in Non-Paper Formats

Reference Number: CTAS-1162

The records of governmental offices are no longer only paper documents or bound books. Records may now be found in a diverse mixture of media. If your office stores records in various formats, such as audiotape or videotape, you may need to make sure some means of accessing the record is readily available to the public. Since the definition of a public record includes records of many formats (including various audio and video records and electronic files), the attorney general has opined that it may violate the Public Records Act if the custodian of the records stored in these other formats could not provide a means for the public to inspect these records.[1] This may require you to have a VCR and television or tape player available for use in your office or somewhere in the courthouse. Separate statutes specifically related to electronic records and microfilm records also require that equipment be available to allow viewing of records stored in these other media.[2]These mandates may be of particular concern to an archives facility which may store records of many different formats in one location. Allowing continued access to these records may prove difficult for both the office that created the records and the archives. For additional information, see Electronic Records.

---

[1] Op. Tenn. Att'y Gen. No. 01-021 (February 8, 2001).

[2] T.C.A. §§ 10-7-121 and 10-7-406.

Providing Access to Electronic or Computerized Records

Reference Number: CTAS-1163

The advent of computers in government record keeping has created legal issues regarding not only the question of "what is a public record?" but also "what is the record itself." If the assessment rolls in the assessor of property's office are stored in computers, is the record only a standard report of that information or is it the raw data itself? If the public requests that the data be organized and produced in a format other than standard reports generated routinely by the office, is it entitled to that information in a format of its own choosing?

This is an area of the law that is developing along with the technology that clouds the issue. While the law was amended in 2017 to mandate acceptance of records request by electronic means under certain circumstances the law is less developed relative to methods of delivering requested records and what electronic data must be provided.

Relative to delivery, the Office of Open Records Counsel (OORC) has stated that when records are maintained electronically, records custodians should produce requested records electronically. The OORC has also stated that records should be produced electronically, when feasible, as a means of utilizing the most economical and efficient method of producing records.

Relative to what electronic data must be provided, under T.C.A. § 10-7-503 a county is not required "to sort through files to compile information or to create or recreate a record that does not exist" and "request for inspection or copying of a public record shall be sufficiently detailed to enable the governmental entity to identify the specific records for inspection and copying." However, the line between simply providing recorded data stored electronically and creating a new record or compiling information can often become blurry based on the request and the county's existing technology resources.

This is an area of the law that will undoubtedly evolve in the coming years as counties and citizens both become increasable intertwined with technology.

Remote Access to Computerized Records

Reference Number: CTAS-1164

Another development that has arisen with the advent of electronic records and the development of the Internet is the ability of citizens to access information remotely. County offices are authorized under Tennessee law to provide computer access and remote electronic access (for inquiry only) to information contained in the records of the office which are stored on computer.[1] Access may be provided both during and after regular business hours. The official who has custody of the records may charge persons using remote electronic access a reasonable amount to recover the costs of providing such services and no other services. The fee must be uniformly applied and must be limited to the actual costs of providing access. It can not include the cost of storage and maintenance of the records or the costs of the electronic record storage system.[2] Any officials providing remote access to their computer records must implement procedures and utilize a system that does not allow records of the office to be altered, deleted or impaired in any manner. Any official choosing to provide this service must file a statement with the office of the Comptroller of the Treasury at least 30 days prior to implementing the system. The statement must describe the computer equipment, software and procedures that are used to provide access and to maintain security and preservation of the computer records. The state of Tennessee will not bear any of the costs of providing access.[3] Once a system for providing access is in place, any member of the public willing to pay the fees must be allowed to have access to the records, including anyone desiring to use the information for proprietary purposes.[4] Similar provisions specific to electronic files of voter registration systems can be found elsewhere in the code.[5]

An attorney general's opinion examined the question of whether a county official could provide remote access to public records through a private vendor.[6] In the circumstances described in the opinion, a vendor was allowed to upload a copy of the data stored on the computers in the office of the register of deeds in exchange for certain services provided by the vendor. The vendor then had the right to provide public access to the data via a subscription service. The attorney general opined that this agreement violated T.C.A. § 10-7-123. Specifically, subsection (a)(4) of that statute provides that once a remote access system is in place, access must be given uniformly to all members of the public who desire access so long as they pay the reasonable fees to the county official to cover the cost of actually providing the service. In this case, remote access was being provided by the county official only to one entity, the vendor, and denied to the rest of the public. The law does not prohibit a private vendor from selling subscriptions to the information which has been acquired from county offices.[7] But it does require the county official to provide equal access to the data to anyone willing to pay the access fee.

The attorney general has also been asked whether there was a problem with the criminal court clerk's office making records, including information about arrests, charges and disposition of cases, available on the Internet. The attorney general opined that the clerk could make such records available in that fashion, so long as the clerk still complied with orders to expunge records and insured they were removed from the Internet as well as the files of the clerk's office once an order compelling expungement was issued by the judge.[8] This standard applied whether a case led to a conviction or was disposed of through judicial diversion.[9]

---

[1] T.C.A. § 10-7-123.
[2] T.C.A. § 10-7-123.
[3] T.C.A. § 10-7-123(a)(1).
[4] T.C.A. § 10-7-123(a)(4).
[5] T.C.A. § 2-2-138.
[6] Op. Tenn. Att'y Gen. No. 04-114 (July 19, 2004).
[7] Op. Tenn. Att'y Gen. No. 04-114.
[8] Op. Tenn. Att'y Gen. No. 00-058 (March 31, 2000).
[9] Op. Tenn. Att'y Gen. No. 00-014 (January 26, 2000).

Denial of Access to Public Records—Liability

Reference Number: CTAS-1165

Any citizen of Tennessee who is denied the right to personal inspection of a public record in whole, or in part, is entitled to petition the court to review the actions that were taken to deny access and to grant access to the record.[1] Petitions may be filed in the chancery court for the county where the records are located or in any other court exercising equity jurisdiction in the county.[2]Upon the filing of the petition, the court shall, at the request of the petitioning party, issue an order requiring the defendant to appear and show cause why the petitioner should not be granted access to the record. No formal written response to the petition is required. The burden of proof rests on the person having custody of the records to show why public access should not be allowed.[3] If the court determines that the petitioner has a right to inspect the records, they shall be made available unless the defendant timely files for appeal or the court certifies a question with respect to disclosure of the records to an appellate court.[4] If a public official is required to disclose records pursuant to these procedures, he or she can not be held civilly or criminally liable for any damages caused by the release of the information.[5] If, however, the court determines that the government entity knowingly and willfully refused to disclose a public record, it may, in the discretion of the judge, assess all reasonable costs involved in obtaining the record, including attorney's fees, against the governmental entity.[6]

---

[1] T.C.A. § 10-7-505(a).
[2] T.C.A. § 10-7-505(b).
[3] T.C.A. § 10-7-505(c).
[4] T.C.A. § 10-7-505(e).
[5] T.C.A. § 10-7-505(f).
[6] T.C.A. § 10-7-505(g).

To What Records Is the Public Entitled Access?

Reference Number: CTAS-1166

It has already been noted that the legislature intended the fullest possible public access to public records. But what are public records? Generally speaking, the courts have ruled that "[i]n those instances where documents have been made or received in connection with the transaction of official business by any governmental agency, then a presumption of openness exists, and the documents are public records

within the meaning of T.C.A.. § 10-7-503."[1] Access is not limited by the format in which the record or information is kept. However, the presumption of openness is overcome whenever state law provides that a record shall be kept confidential.

---

[1] *Griffin v. City of Knoxville*, 821 S.W.2d 921, 924 (Tenn. 1991) as quoted in Op. Tenn. Att'y Gen. No. 99-011 (January 25, 1999).

Confidential Records

Reference Number: CTAS-1167

A lengthy statute in the Tennessee Public Records Act provides a laundry list of government records that must be kept confidential.[1] This statute is amended and added to on a regular basis by the General Assembly. The following list highlights a few of the many records designated as confidential by T.C.A. § 10-7-504 (see statute for complete list):

- Medical records of patients in state, county, and municipal hospitals and medical facilities;
- Any records concerning the source of body parts for transplantation or any information concerning persons donating body parts;
- All investigative records of the TBI, the office of the TennCare inspector general, all criminal investigative files of the motor vehicle enforcement division of the department of safety relating to stolen vehicles or parts, all files of the drivers' license issuance division and the handgun carry permit division of the department of safety relating to bogus drivers' licenses and handgun carry permits issued to undercover law enforcement agents;
- Records of students in public educational institutions (for more discussion of these records, see Student Records);
- Certain books, records, and other materials in the possession of the office of the attorney general relating to any pending or contemplated legal or administrative proceeding;
- State agency records containing opinions of value or real and personal property intended to be acquired for a public purpose;
- Certain personal information of law enforcement officers[2];
- Investigative records and reports of the internal affairs division of the department of correction or the department of children's services;
- Official health certificates, collected and maintained by the state veterinarian;
- The capital plans, marketing information, proprietary information, and trade secrets submitted to the Tennessee venture capital network;
- Records of historical research value which are given or sold to public archival institutions, public libraries, or libraries of a unit of the board of regents or the University of Tennessee, when the owner or donor wishes to require that the records are kept confidential;
- Personal information contained in motor vehicle records;
- All memoranda, work notes or products, case files, and communications related to mental health intervention techniques conducted by professionals in a group setting to provide job-related critical incident counseling and therapy to law enforcement officers, EMTs, paramedics, and firefighters;
- All riot, escape, and emergency transport plans incorporated in a policy and procedures manual of county jails and workhouses or prisons operated by the department of correction or under private contract;
- In order of protection cases, any documents required for filing other than certain forms promulgated by the Tennessee Supreme Court;
- Computer software and manuals sold to state agencies or counties;
- Credit card numbers and related identification numbers or authorization codes;
- Credit card numbers, social security numbers, tax ID numbers, financial institution account numbers, burglar alarm codes, security codes, and access codes of any utility;
- Records that would allow a person to identify areas of structural or operational vulnerability of a utility service provider or that would permit disruption or interference with service;

- Contingency plans of governmental entities for response to violent incidents, bomb threats, ongoing acts of violence, threats related to weapons of mass destruction, or terrorist incidents;
- Records of any employee's identity, diagnosis, treatment, or referral for treatment by a state or local government employee assistance program;
- Unpublished telephone numbers in the possession of emergency communications districts;
- Personally identifying information ((i) Social security numbers; (ii) Official state or government issued driver licenses or identification numbers; (iii) Alien registration numbers or passport numbers; (iv) Employer or taxpayer identification numbers; (v) Unique biometric data, such as fingerprints, voice prints, retina or iris images, or other unique physical representations; or (vi) Unique electronic identification numbers, addresses, routing codes or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data;
- Records identifying a person as being directly involved in the process of executing a sentence of death; and
- Information that would allow a person to obtain unauthorized access to confidential information or to government property. [3]

For county governments, one important class of confidential records involves personal information of state, county, municipal, and other public employees. An employee's home telephone and personal cell phone numbers, bank account information, health savings account information, retirement account information, pension account information, Social Security number, residential address, driver's license information (except where driving is a part of the employee's job), emergency contact information, and personal, non-government issued, email address are confidential. Additionally, applicants for county employment and former employees are also protected by these confidentiality provisions (as are immediate family members, whether or not the immediate family member resides with the employee, or household members of the employee). Where this confidential information is part of a file or document that would otherwise be public information, such information shall be redacted if possible so that the public may still have access to the nonconfidential portion of the file or document. T.C.A. § 10-7-504(f).

Proposals and statements of qualifications received by a local government entity in response to a personal service, professional service, or consultant service request for proposals or request for qualifications solicitation, and related records, including, but not limited to, evaluations, names of evaluation committee members, and all related memoranda or notes, are declared to be confidential, but only until the intent to award the contract to a particular respondent is announced. T.C.A. § 10-7-504(a).

This list of confidential records found in T.C.A. § 10-7-504 is not exclusive, however, and other statutes, rules, and the common law dealing with a subject matter can also make a specific record confidential.[4] While the following list is not exhaustive, these statutes are other legal sources that designate certain records that may be in the possession of a county office as confidential:

- All memoranda, work products or notes and case files of victim-offender mediation centers (T.C.A. § 16-20-103);
- Adoption records and related records (T.C.A. §§ 36-1-102 and following);
- Many records regarding juveniles (see T.C.A. §§ 37-1-153, 37-1-154, 37-1-155, 37-1-409, 37-1-612, 37-1-615 and 37-2-408);
- Certain records regarding the granting of consent to abortion for a minor and other records regarding abortion (T.C.A. §§ 37-10-304, 39-15-201);
- Pursuant to T.C.A. § 38-7-110, all or a portion of a county medical examiner's report, toxicological report or autopsy maybe declared confidential upon petition by the district attorney on the grounds that release of such record could impair the investigation of a homicide or felony. Additionally, 2005 Public Chapter 216 made it a criminal offense for certain audio and video materials related to an autopsy to be release to an unauthorized person.
- Certain student information;
- Whistleblowing reports of violations the Education Trust in Reporting Act (T.C.A. §§ 49-50-1408);
- Certain records of an employer's drug testing program (T.C.A. § 50-9-109);
- Accident reports (T.C.A. § 55-10-114 (along with 10-7-504));
- Tax returns and tax information (T.C.A. § 67-1-1702);

- Business tax statements, reports, and returns as well as some information on business license applications[5](T.C.A. § 67-4-722);
- Information or records held by a local health department regarding sexually transmitted diseases (T.C.A. § 68-10-113);
- Patient medical records of hospitals and local or regional health departments (T.C.A. § 68-11-305); and
- Nursing home patient records (T.C.A. § 68-11-804).

Please note that this list only highlights some of the other provisions of the Tennessee Code that make records confidential. Additionally, the Tennessee Supreme Court has ruled that sources of legal authority other than statutes may make a record confidential. For example, the Tennessee Supreme Court has ruled that the Tennessee Rules of Criminal Procedure and Civil Procedure may also designate certain records as confidential.[6] Other records may be sealed by a court order or made confidential by a federal statute or regulation. If you have a question regarding the confidentiality of a specific record not listed above, contact your county attorney or CTAS county government consultant for assistance.

---

[1] T.C.A. § 10-7-504.

[2] T.C.A. § 10-7-503(c) also addresses the subject.

[3] T.C.A. § 10-7-504.

[4] Op. Tenn. Att'y Gen. No. 99-022 (February 9, 1999).

[5] See Op. Tenn. Att'y Gen. No. 01-165 (September 15, 2001) for a discussion of the confidentiality of phone numbers and other identifying numbers used in the enforcement of the business tax.

[6] See. *Appman v. Worthington*, 746 S.W.2d 165, 166 (Tenn. 1987) and Ballard v. Herzke, 924 S.W.2d 652, 662 (Tenn. 1996).

Maintenance of Confidentiality

Reference Number: CTAS-1168

Any record that is designated as confidential must be treated as confidential by the agency with custody of the record throughout the maintenance, storage, and disposition of the record. This includes destroying the record (if it is eligible for destruction) in such a manner that the record cannot be read, interpreted, or reconstructed[1]. However, once a confidential record has been in existence more than 70 years, it shall be open for public inspection by any person unless disclosure of the record is specifically prohibited or restricted by federal law or unless the record is a record of services for mental illness or retardation.[2] This "70-year rule" also does not apply to adoption records, records maintained by the office of vital records, and records of the TBI that are confidential.[3]

---

[1] T.C.A. § 10-7-504(b). See also Op. Tenn. Att'y Gen. 01-040 (March 19, 2001).

[2] T.C.A. § 10-7-504(c).

[3] T.C.A. § 10-7-504(c).

Special Considerations and Specific Types of Confidential Records

Reference Number: CTAS-1169

Personally Identifying Information

Reference Number: CTAS-1170

In 2016 the General Assembly amended T.C.A. § 10-7-504 to provide that no governmental entity shall publicly disclose *personally identifying information* of any citizen of the state unless: (i) Permission is given by the citizen; (ii) Distribution is authorized under state or federal law; or (iii) Distribution is made: (*a*) To a consumer reporting agency as defined by the federal Fair Credit Reporting Act (15 U.S.C. §§ 1681 et seq.); (*b*) To a financial institution subject to the privacy provisions of the federal Gramm Leach Bliley Act (15 U.S.C. § 6802); or (*c*) To a financial institution subject to the International Money Laundering Abatement and Financial Anti–Terrorism Act of 2001 (31 U.S.C. §§ 5311 et seq.).

The law defines "personally identifying information" to include: (i) Social security numbers; (ii) Official state or government issued driver licenses or identification numbers; (iii) Alien registration numbers or passport numbers; (iv) Employer or taxpayer identification numbers; (v) Unique biometric data, such as fingerprints, voice prints, retina or iris images, or other unique physical representations; or (vi) Unique electronic identification numbers, routing codes or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data.

The law provides that it does not prohibit the use of personally identifying information by a governmental entity in the performance of its functions or the disclosure of personally identifying information to another governmental entity, or an agency of the federal government, or a private person or entity that has been authorized to perform certain duties as a contractor of the governmental entity.

The name, mailing address, physical address, phone number, email address, social security number, or any other personally identifying information provided by an individual, whether or not the individual is a citizen of this state, as part of the individual's use of, or participation in, a government-sponsored or -supported property alert service or program, is not a public record and is not open for public inspection. "Property alert service or program" refers to an online service that electronically alerts participants when a document is filed and indexed in the register of deed's office that references the participant's name or address.

Motor Vehicle Registration Records

Reference Number: CTAS-1171

Access to motor vehicle registration records held by the Department of Safety, the Department of Revenue, or in the office of the county clerk when acting as an agent of those departments is restricted by both state and federal law. The federal Drivers Privacy Protection Act places restrictions on access to these records.[1] In addition, in 1996, our state legislature adopted the Uniform Motor Vehicle Records Disclosure Act that closely parallels the language of the federal act.[2] Under the provisions of these laws, personal information obtained by those government offices in connection with a motor vehicle record can not be disclosed except for specific purposes to certain authorized individuals or with the consent of the driver.[3] Personal information is defined to include information that identifies a person, including an individual's photograph, computerized image, social security number, driver identification number, name, address, telephone number, and medical or disability information.[4] Use of the information is generally allowed for governmental agencies in carrying out their functions.[5] Additionally, the statutes include about a dozen other authorized uses whereby certain private parties have rights to access the records for those specified purposes.[6] If a county clerk is presented with a request for personal information from motor vehicle records from a private citizen or a company, he or she should compare the request to the restrictions and authorizations found in T.C.A. §§ 55-25-103 through 55-25-112 and 18 U.S.C. § 2721 through 18 U.S.C. § 2725 to determine whether the release of such information is lawful. The Tennessee Department of Safety, Division of Title and Registration may be able to provide county clerks with further guidance regarding these records if necessary.

---

[1] 18 U.S.C. § 2721 through § 2725.

[2] T.C.A. §§ 55-25-101, *et seq.*

[3] T.C.A. §§ 55-25-104 through 55-25-107 and 18 U.S.C.A. § 2721.

[4] T.C.A. § 55-25-103(6).

[5] 18 U.S.C. § 2721(b)(1) and T.C.A. § 55-25-107.

[6] 18 U.S.C. § 2721 and T.C.A. § 55-25-105 through 107.

Vital Records

Reference Number: CTAS-1172

To protect the integrity of vital records and to insure their proper use and the proper administration of those records, the General Assembly made it unlawful for a custodian of these records to permit inspection of, or to disclose information contained in vital records, or to copy or issue a copy of all or part of any such records except in strict accordance with procedures found in the law or in accordance with a court order.[1] But the law goes on to state that an application for a marriage license and the authenticating documentation for the events of birth, death, marriage, divorce or annulment of a marriage, in the possession of a county clerk, court clerk, state registrar, or other authorized custodian are public records and that verified information from such documents may be provided upon request. However, the information contained in the "Information for Medical and Health Use Only" section of a birth certificate and the "Confidential Information" section of marriage, divorce, or annulment certificates remains confidential.[2]

---

[1] T.C.A. § 68-3-205.
[2] T.C.A. § 68-3-205(d).

Law Enforcement Personnel Records

Reference Number: CTAS-1173

A couple of specific statutory provisions provide extra protection to personnel records of law enforcement personnel. Under T.C.A. § 10-7-503(c), there are requirements that when personnel records of law enforcement officers are inspected, the custodian of the records must make a record of the inspection and inform the officer. The person wishing to inspect the records must provide his or her name, address, business telephone number, home telephone number, driver license number, or other appropriate identification prior to receiving access to the records. Within three days after the inspection, the officer whose files have been examined should be informed that the inspection has taken place; the name, address, and telephone number of the person making the inspection; for whom the inspection was made; and the date of the inspection.[1]

In addition, T.C.A. § 10-7-504(g) provides that the personnel information of law enforcement personnel shall be redacted where there is a reason not to disclose the information as determined by the sheriff or the sheriff's designee. When a request to inspect includes personal information and the request is for a professional, business, or official purpose, the sheriff or custodian shall consider the specific circumstances to determine whether there is a reason not to disclose and shall release all information, except information made confidential in T.C.A. § 10-7-504(f), if there is not such a reason. In all other circumstances, the officer shall be notified prior to disclosure of the personal information and shall be given a reasonable opportunity to be heard and oppose the release of the information. In addition to the requirements of T.C.A. § 10-7-503(c), the request for a professional, business, or official purpose shall include the person's business address, business telephone number and email address. The request may be made on official or business letterhead and the person making the request shall provide the name and contact number or email address for a supervisor for verification purposes. If the sheriff, the sheriff's designee, or the custodian of the information decides to withhold personal information, a specific reason shall be given to the requestor in writing within two (2) business days, and the file shall be released with the personal information redacted. For purposes of T.C.A. § 10-7-504(g), personal information shall include the officer's residential address, home and personal cellular telephone number; place of employment; name, work address and telephone numbers of the officer's immediate family; name, location, and telephone number of any educational institution or daycare provider where the officer's spouse or child is enrolled.

In addition to the provisions relative to the office's residential address in T.C.A. § 10-7-504(g), subsection (f) of the same statute provides that the residential address of a law enforcement officer held by the county in its capacity as an employer shall be confidential and any person who releases the information commits a Class B misdemeanor if the person acts with criminal negligence, or a Class A misdemeanor if the person knows the information is to be treated as confidential and intentionally releases the information to the public.

Finally, T.C.A. § 10-7-504(g) also provides that the sheriff may segregate information that could be used

to identify or to locate an officer designated as working undercover.[2]

---

[1] T.C.A. § 10-7-503(c).
[2] T.C.A. § 10-7-504(g).

Computerized Data Breaches

Reference Number: CTAS-2204

Under T.C.A. § 47-18-2901 counties must create safeguards to ensure the security of personal information on laptop computers and other removable storage devices. Failure to comply with this requirement creates a cause of action against the county if identity theft results. Also, T.C.A. § 47-18-2107 requires any holder of computerized personal information that is confidential to disclose any breach of the security of the system to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Domestic Violence Prevention and Protection Documents

Reference Number: CTAS-1174

In addition to the large group of records made strictly confidential by state laws, there is another class of records that *may* be made confidential by a 1999 law. Chapter 344 of the public acts of 1999 amends T.C.A. § 10-7-504 to allow persons who have obtained a "valid protection document" to request certain information that could be used to locate them be kept confidential. Protection documents are defined by the act and include such things as orders of protection and affidavits of directors of a rape crisis center or domestic violence shelter. If the individual desiring confidentiality presents one of these documents to the records custodian for the governmental entity and requests confidentiality, the custodian of the records may choose to comply with the request or reject it. If the request is rejected, the custodian must state the reason for denying the request. If the request is granted, the records custodian must place a copy of the protection document in a separate confidential file with any other similar requests, indexed alphabetically by the names of the persons requesting confidentiality. From that point on until the custodian is notified otherwise, any time someone requests to see records of the office, the records custodian must consult the file and ensure that any identifying information about anyone covered by a protection document filed with the office is kept confidential before allowing any record to be open for public inspection. "Identifying information" includes any record of the home and work addresses, telephone numbers, social security number and "any other information" regarding the person that could reasonably be used to locate an individual. That information must be redacted from the records of the office before anyone can be allowed to inspect the records of the office. Since it is difficult to ascertain what information could possibly be used to locate an individual, you are strongly cautioned against complying with such requests. Unless you are certain your office can redact all identifying information regarding an individual from all files of your office you should probably reject such requests for confidentiality, citing the administrative difficulty in redacting the records. It is not mandatory for your office to comply with these requests. However, if you do comply and then fail to protect all such information, you may create liability for your office.

County Hospital and Health Department Records and Ambulance Records

Reference Number: CTAS-1175

Special rules apply to medical records. They are governed primarily by T.C.A. §§ 68-11-301 and following. The definition of hospital used in those provisions is broad enough to include county health departments.[1] Certain hospital records are not public records.[2] Generally, the law requires that a hospital or health department is required to retain and preserve records which relate directly to the care and treatment of a patient for 10 years following the discharge of the patient or such patient's death during the period of treatment within the hospital.[3] Mental health records are treated differently. Hospitals and health departments are given the option of retaining records for a longer period of time if they wish.[4] Records held by a local health department related to sexually transmitted diseases are

strictly confidential.[5]

Records of ambulance services are similar in some respects to hospital records. There are a handful of statutes and regulations that specifically mandate the creation and retention of certain records related to the operation of ambulance services.[6] The information in run records that relates to the medical condition and treatment of the patient is specifically declared confidential.[7] Although the statutes and regulations do not establish retention period for all ambulance records, it is recommended that ambulance services should follow the general standard of a 10-year retention period for records that are medical in nature. Additionally, the rules of the Emergency Medical Services Division specifically require that ambulance dispatch logs should be retain for at least 10 years.[8]

---

[1] T.C.A. § 68-11-302.

[2] T.C.A. § 68-11-304.

[3] T.C.A. § 68-11-305.

[4] T.C.A. § 68-11-307.

[5] T.C.A. § 68-10-113.

[6] See T.C.A. §§ 68-140-301, *et seq.*, especially § 68-140-319 and the official Rules of the Tennessee Department of Health, Bureau of Manpower and Facilities, Emergency Medical Services Division, Rules 1200-12-1-.05, 1200-12-1-.09 and 1200-12-1-.15.

[7] T.C.A. § 68-140-319.

[8] Rules of the Emergency Medical Services Division, Rules 1200-12-1-.15.

HIPAA

Reference Number: CTAS-1176

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, is a federal law that instituted dramatic reforms regarding the use of information in the health care and insurance industry. It created a great deal of apprehension among many private and public entities that were uncertain about whether the act impacted them as well. The Act required the Secretary of Health and Human Services to issue privacy regulations governing individual health care information. The privacy provisions of HIPAA are found in the ironically named "administrative simplification" provisions of the act. The goal of the privacy rule is to safeguard protected health information (PHI) while allowing the free flow of health care information in the world of electronic commerce and transactions.[1] Protected health information includes all individually identifiable health information held by a covered entity or its business associate in any form or media.[2] In other words, it is made up of health and medical records that identify the individual to whom the record relates. The privacy rules apply to three types of entities: health plans, health care providers, and health care clearinghouses.[3] The easiest category to consider from the local government standpoint is the health care clearinghouse. This category deals with entities that process and re-format information being transmitted between entities. Counties will not fall under this category.

Health plans are individual and group health care plans that provide or pay the cost of medical care.[4] If your county provides health insurance for its employees through private insurance, the insurance carrier would be the health plan. If your county is self-insured, it is likely that in administering the self-insured health care plan, the county will have to comply with the privacy rules and may be covered by HIPAA. If you have a third party administrator, that entity may be handling most compliance issues for the county, but you should still evaluate your requirements under HIPAA. Technically your third party administrator is merely a "business associate" under the terms of HIPAA who falls under provisions of the law due to its relationship with the county's health plan. Responsibility for compliance ultimately lies with the plan itself and not with its business associates.

Health care providers are also be covered by HIPAA if the provider electronically transmits health information in connection with certain types of transactions.[5] These include claims, benefit eligibility inquiries, referral authorization requests, or certain other transactions listed under the HIPAA Transactions Rule.[6] For example, the fact that your county may employ a nurse or doctor for the jail may make the county a health care provider; however, the county will only be a *covered* health care provider under HIPAA if those employees are electronically transmitting health information in conjunction with one of the

listed transactions. If your sheriff does not employ personnel to provide medical services to the jail but merely contracts with another entity to provide the service, then the sheriff's office would not be a covered entity.

Even if it appears that some aspects of county government may be considered covered functions under certain circumstances, it is possible for the county to declare itself a hybrid entity. Under the HIPAA regulations, a hybrid entity is a single legal entity that is covered, but whose covered functions are not its primary functions.[7] By being declared a hybrid entity, the county limits the application of the HIPAA requirements to only those county operations that are acting as a health care provider. For instance, a county operated ambulance service or hospital would need to comply with HIPAA as a health care provider if it transmits PHI electronically, but the register of deeds and county clerk's offices, and other non-health care operations would not be covered.

Covered entities are required to provide notices and disclosures to individuals who have PHI held by the entity. If you have been to a doctor's office in the last couple of years, you have probably seen these standard forms. Offices that are covered by HIPAA are also required to adopt privacy policies and procedures that are consistent with the privacy rule, must designate a privacy official responsible for implementing these policies, must conduct workforce training and management, must mitigate any harmful disclosures of PHI, must maintain reasonable appropriate safeguards to protect against improper disclosure of PHI, must have procedures for receiving complaints about privacy issues, and must meet certain documentation and record keeping standards.[8]

The HIPAA rules and regulations are extremely complex and filled with exceptions, limitations, and modifications for various entities and transactions and will only apply to limited operations of local governments if at all. If you think your office or your county may be covered by HIPAA, you should discuss the requirements of the law with your county attorney and with any third party administrators or other health care consultants with which your county may contract. For more information about the law and associated rules, see the Web site for the HHS, Health Information Privacy. A recent opinion of the Tennessee attorney general also gives instructions with regard to the release of health information under HIPAA for law enforcement purposes.[9]

---

[1] Department of Health and Human Services, Office for Civil Rights HIPAA Privacy Rule Summary

[2] 45 C.F.R. § 164.501.

[3] 45 C.F.R. § 160.102.

[4] 45 C.F.R. §§ 160.102 and 160.103.

[5] 45 C.F.R. § 160.102.

[6] 45 C.F.R. Part 162.

[7] 45 C.F.R. § 164.504.

[8] 45 C.F.R. § 164.530.

[9] Op. Tenn. Att'y Gen. 04-153 (October 7, 2004).

Credit Card Numbers and Credit Reports

Reference Number: CTAS-1177

As county governments have begun allowing citizens to use credit cards for payment of taxes and fees, government records keepers encounter some new regulations and challenges in managing records that contain information related to those credit accounts. Credit card numbers of persons using an account to make payments to the government are confidential under T.C.A. § 10-7-504(a)(19). Additionally, there are notification requirements that apply when a breach of security has allowed improper access to electronic account information or other personal information that could be used for identity theft purposes.

Finally, local governments that use credit reports as a part of background checks must comply with the Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act (FACTA) and related rules and regulations of the Federal Trade Commission[1]. The FCRA requires employers that use private agencies to perform background checks (whether related to credit history, criminal background or driving record checks) on job applicants to comply with notice, consent, and disclosure requirements related to such checks and reports. FACTA added the requirement that entities possessing

consumer information related to these reports must properly dispose of such information in a manner that preserves confidentiality and requires those possessing such information to take reasonable measures to ensure against unauthorized access or use of the information. Therefore, if your county uses private reporting agencies for background checks during the employment process or for other purposes, make sure anyone in your county possessing this information properly protects this sensitive consumer information.

---

[1] Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952 with related regulations found in 16 CFR Part 682.

Source URL: *https://www.ctas.tennessee.edu/eli/public-access-records*